UNITED STATE DISTRICT COURT
DISTRICT OF NEBRASKA

JOHN SIEBUHR, *individually and on behalf of all others similarly situated*; *Plaintiff,* v. ALN MEDICAL MANAGEMENT, LLC, *Defendants*.	)	**Civil Action No.: 4:25-cv-3077** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

ORIGINAL COMPLAINT—CLASS ACTION

Plaintiff John Siebuhr ("Plaintiff"), individually and on behalf of all others similarly situated, sues Defendant ALN Medical Management, Inc. ("ALN" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information"), of Plaintiff and other current and former patients of Defendant's clients, the putative class members ("Class"). This Data Breach occurred between March 18, 2024, and March 24, 2024.

2. ALN is a provider of outsourced revenue cycle management services for independent physicians that is headquartered in Lincoln, Nebraska.[1]

3. The Private Information compromised in the Data Breach included certain PII and PHI of Defendant's client's current and former patients, including Plaintiff. This Private Information included but is not limited to "name, date of birth, address, Social Security number, driver's license number, passport number, other government-issued identification number, financial account information, payment card information, and medical information, including medical record numbers, health insurance information, claims data, and diagnosis and treatment information."[2]

4. Defendant has reported to the Office of the Texas Attorney General that the Private Information of 127,112 individual Texans was affected in the data breach.[3]

5. The Private Information was acquired by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals.

6. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which they were entrusted.

7. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and

---

[1] ALN Revenue Cycle Management, Home, https://alnmm.com/ (last visited April 2, 2025).
[2] ALN., *Cyber Security Incident Notice*, *available at*: https://alnmm.com/home/notice-of-cyber-security-event/ (last visited April 2, 2025)
[3] State of Texas, Office of the Attorney General, Data Security Breach Report, *available at* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited April 2, 2025)

other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what specific type of information was accessed.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

9. Defendant, through its employees, disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions.

10. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

11. In addition, Defendant's employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

12. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

13. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

18. Accordingly, Plaintiff sues Defendant seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence per se, (iii) breach of implied contract, and (iv) breach of fiduciary duty.

II. PARTIES

19. Plaintiff John Siebuhr is and at all times mentioned herein was an individual citizen of New York, residing in the city of Mount Vernon.

20. Plaintiff provided his trusted Private Information to his medical provider who in turn provided Plaintiff's Private Information, including PII and PHI, to Defendant for administrative purposes.

21. Plaintiff received notice of the Data Breach around March 21, 2025, informing him that his sensitive information was part of Defendant's Data Breach. See Exhibit A.

22. Defendant ALN is a Nebraska domestic medical billing and claims processing corporation, with its principal place of business located at 4433 S 70th St Ste 100 Lincoln, Nebraska 68516.[4]

23. Defendant can be served through its registered agent, Julie A. Huffman in person at the same location.[5]

III. JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs. Upon information and belief, the number of Class Members is over 100,000, many of whom have different citizenship from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

---

[4] Nebraska Secretary of State, Corporate & Business Search, available at: https://www.nebraska.gov/sos/corp/corpsearch.cgi?acct-number=1118277 (*last accessed*: April 2, 2025).
[5] I*d.*

25. This Court has general personal jurisdiction over defendant because it is an entity based and operating in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this district.

26. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because Defendant maintains its principal place of business within the District of Nebraska and because a substantial part of the acts or omissions giving rise to this action occurred within this District.

IV. FACTUAL ALLEGATIONS

A. DEFENDANT'S BUSINESS

27. ALN is a provider of outsourced revenue cycle management services for independent physicians that is headquartered in Lincoln, Nebraska.[6]

28. The Defendant's services include billing, coding insurance AR follow-up and denial management as well as the implementation of practice management and medical record systems.[7]

29. Defendant provides those services to medical providers, including National Spine and Pain, Inpatient Physician Associates, LLC, Hoag Clinic, and Allied Physicians Group.

30. In the ordinary course of business, and in order to gain profits, Defendant required the medical providers used by Plaintiff and Class members to provide (and Plaintiff did provide to his medical providers) Defendant with sensitive, personal, and private information, such as his or her:

- Name;
- Date of Birth;
- Address;

[6] ALN Revenue Cycle Management, Home, https://alnmm.com/ (last visited April 2, 2025).
[7] *Id.*

- Health Insurance Information;
- Medical Information; and
- Demographic Information

31. All of Defendant's employees, staff, entities, sites, and locations may share patient protected health information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendant is required to maintain.

32. Upon information and belief, Defendant's HIPAA Privacy Policy is provided to every patient, via the patient's medical provider prior to receiving healthcare services, and upon request.

33. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it, via medical providers, by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable contractual obligations, laws, regulations including the Health Insurance Portability and Accountability Act ("HIPAA"), and common law.

34. The patient protected health and personal information held by Defendant in their computer systems and networks included the Private Information of Plaintiff and Class Members.

B. THE DATA BREACH

35. A Data Breach typically occurs when cyber criminals who intend to and successfully act to access and steal Private Information that has not been adequately secured by business entities like Defendant.

36. The Cyber Security Incident Notice published on Defendant's website states in part:

> In March 2024, ALN identified suspicious activity related to certain systems being hosted by a third-party service provider. Upon learning of this activity, ALN promptly took steps to ensure the security of ALN systems, isolated the impacted environment, and launched an investigation to determine the nature and scope of the activity. While this incident did not impact internal ALN systems, the investigation determined that certain files and folders within ALN's third-party hosted environment were accessed or taken by an unauthorized actor between March 18, 2024 and March 24, 2024. As a

> result, ALN began an extensive programmatic and manual review of these files and folders to determine whether sensitive data related to individuals associated with certain ALN clients received through the ordinary course of business for the provision of services to these clients. Although the information varies for each individual, the potentially impacted data includes: name, date of birth, address, Social Security number, driver's license number, passport number, other government-issued identification number, financial account information, payment card information, and medical information, including medical record numbers, health insurance information, claims data and diagnosis and treatment information. [8]

37. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[9] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HHS.[10]

38. Defendant cannot claim it was unaware of the HHS notification requirements as it complied (at least in part) with those requirements.

39. Plaintiff's notice letter was dated March 21, 2025 —more than one year after Defendant discovered the Data Breach.

40. Defendant had obligations created by HIPAA, contract, industry standards, state law, common law, and representations made to Plaintiff and Class Members, to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

---

[8] ALN., *Cyber Security Incident Notice*, *available at*: https://alnmm.com/home/notice-of-cyber-security-event/ (last visited April 2, 2025)

[9] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed April 2, 2025).

[10] *Id*.

41. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

42. Defendant's data security obligations were particularly important given the substantial increase in Data Breaches targeting personal identifying information preceding the date of the breach.

43. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[11] Of the 2023 recorded data breaches, 809 of them, or 25% were in the medical or healthcare industry.[12] The 809 reported breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breach that exposed just over 28 million sensitive records in 2022. [13]

44. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

45. In fact, according to the cybersecurity firm Mimecase, 90% of health care organization experienced cyberattacks in the past year.[14]

46. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public, including Defendant.

---

[11] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited April 2, 2025).
[12] *Id*.
[13] *Id*. at 11, Fig. 3.
[14] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), *available at* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited March 5, 2025).

C. DATA BREACHES ARE PREVENTABLE

47. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

48. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

49. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[15]

50. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and

[15] How to Protect Your Networks from RANSOMWARE, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[16]

51. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts
- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene
- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege
- Monitor for adversarial activities

[16] *Id.* at 3-4.

- Hunt for brute force attempts
- Monitor for cleanup of Event LogsAnalyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[17]

52. Given that Defendant was storing the Private Information of its client's current and former patient Defendant could and should have implemented all the above measures to prevent and detect cyberattacks.

53. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiffs and Class Members.

D. DEFENDANT ACQUIRES, COLLECTS & STORES MEMBERS' PRIVATE INFORMATION

54. Defendant acquires, collects, and stores a massive amount of Private Information on its client's current and former patients.

55. As a condition of becoming a patient with a medical provider who is a client of Defendant, patients are required to entrust Defendant with highly sensitive personal information

56. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

---

[17] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last viewed April 2, 2025).

57. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

58. Upon information and belief, while collecting Private Information from patients, including Plaintiff, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

59. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

E. VALUE OF PRIVATE INFORMATION

60. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id.*

61. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[20]

62. For example, Personal Information can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

63. Theft of PHI is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[23]

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft.

---

[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last viewed April 2, 2025)

[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last viewed March 27, 2025)

[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last viewed April 2, 2025)

[23] Medical I.D. Theft, FraudPrevention, available at https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited February 17, 2025).

> Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

F. DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

67. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

68. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal Private Information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[25] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[26]

---

[24] *Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf*

[25] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 26, 2025).

[26] *Id.*

69. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect client patient data, by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

71. These FTC enforcement actions include actions against defendants that failed to properly implement basic data security practices.

72. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.Defendant were always fully aware of its obligation to protect the PII of its members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

73. As shown above, experts studying cyber security routinely identify corporations that maintain PII data as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

74. Several best practices have been identified that a minimum should be implemented by Defendant, including, but not limited to, educating all employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti- malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

75. Other best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

76. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

77. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

H. DEFENDANT'S CONDUCT VIOLATES HIPAA AND REVEALS ITS INSUFFICIENT DATA SECURITY

78. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

79. Covered entities must implement safeguards to ensure the confidentiality, integrity and availability of PHI. Safeguards must include, physical, technical, and administrative components.

80. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include: 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. §164.312(a)(1); 45 C.F.R. § 164.308(A)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

81. A Data Breach such as the one Defendant 3experienced is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule. *See* 45 C.F.R. 164.402 (Defining "Breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.")

82. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to meet standards mandated by HIPAA regulations.

V. DEFENDANT'S BREACH

83. Defendant breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

k. Failing to train all members of Defendant's workforce effectively on the policies and procedures about PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

l. Filing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption")

m. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

o. Failing to adhere to industry standards for cybersecurity; and

p. Failing to provide notice once the scope of the breach was determined.

84. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

85. As the result of computer systems needing security upgrading, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

86. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

B. PLAINTIFF AND THE CLASS MEMBERS HAVE AND WILL EXPERIENCE SUBSTANTIAL HARM IN THE FORM OF RISK OF CONTINUED IDENTITY THEFT.

87. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

88. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

89. Because of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and consequences of the Data Breach, including, but not limited to, efforts spent

researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies; Unauthorized use of stolen PII; and

g. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

90. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

91. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals often post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

92. It can take victims years to spot identity or PII theft, giving criminals plenty of time to abuse that information for money.

93. One such example of criminals using PII for profit is the development of "Fullz" packages.

94. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

95. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers,

email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is traceable to the Data Breach.

96. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims, and the numbers are only rising.

97. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

98. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

99. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their

reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

100. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

101. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[27]

102. The FTC has also issued many guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires:

a. encrypting information stored on computer networks;

b. retaining payment card information only as long as necessary;

c. properly disposing of personal information that is no longer needed;

d. limiting administrative access to business systems;

e. using industry-tested and accepted methods for securing data;

f. monitoring activity on networks to uncover unapproved activity;

g. verifying that privacy and security features function properly;

h. testing for common vulnerabilities; and

i. updating and patching third-party software.

[27] Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009).

103. According to the FTC, unauthorized PII disclosures ravage consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[28] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

104. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

105. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

C. DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTITY THEFT

106. Data Breaches such as the one experienced by Defendant's client's current and former patients are especially problematic because of the disruption they cause to the daily lives of victims affected by the attack.

107. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[29]

108. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit

---

[28] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited March 27, 2025).

[29] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited March 27, 2025) ("GAO Report").

bureaus to place a fraud alert (possibly an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[30]

109. Identity thieves use stolen personal information such as Social Security numbers for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

110. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

111. Theft of Private Information is gravely serious. PII/PHI is a valuable property right.[31]

112. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

113. Theft of PHI is also gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and

---

[30] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited March 27, 2025).

[31] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

payment records, and credit report may be affected." Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves.

114. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

115. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

116. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

117. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[32] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

118. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for more credit lines.[33] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[34] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

119. It is also hard to change or cancel a stolen Social Security number.

120. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

---

[32] Ashiq Ja, *Hackers Selling [healthcare] Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-[healthcare]-data-in-the-black-market/ (last visited March 27, 2025).
[33] Social Security Administration, *Identity Theft and Your Social Security Number* (2018), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited March 27, 2025).
[34] *Id* at 4.
[35] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (February 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying- about-identity-theft (last visited April 2, 2025).

121. Healthcare data, as one would expect, demands a much higher price on the black market. The National Association of Healthcare Access Management reports,"[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[36]

122. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[37]

123. In recent years, the corporations that maintain medical and financial data in their network systems have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant were put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

VI. PLAINTIFF'S EXPERIENCE

124. Plaintiff John Siebuhr is and at all times mentioned herein was an individual citizen of New York, residing in the city of Mount Vernon.

125. Plaintiff provided Defendant with his sensitive PII to obtain healthcare as a patient of Defendant's client.

126. On March 21, 2025, Defendant mailed Plaintiff and Class Members a Notice that stated in part:

What Happened

---

[36] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited April 2, 2025).

[37] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for- everyone/ (last visited April 2, 2025).

> In March 2024, ALN identified suspicious activity related to certain systems being hosted by a third-party service provider. Upon learning of this activity, we promptly took steps to ensure the security of our systems, isolated the impacted environment, and launched an investigation to determine the nature and scope of the activity. The investigation determined that certain files and folders within our third-party hosted environment were accessed or taken by an unauthorized actor between March 18, 2024 and March 24, 2024…
>
> **What Information Was Involved**
> Our review determined that information related to certain individuals was present in the involved files and folder. Following this determination, we undertook an in-depth review process to identify the individuals and ALN clients who were potentially impacted and notified Allied Physicians Group. ALN is notifying you now out of an abundance of caution because the information involved in this incident includes your Date of birth, Health Insurance Information, Medical Information, Demographic Information, and name.[38]

127. Plaintiff stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents.

128. Moreover, Plaintiff diligently chooses unique usernames and passwords for his sensitive online accounts.

129. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted his personal data to Defendant.

130. Because of the Data Breach, Defendant advised Plaintiff to take certain steps to protect his Private Information and otherwise mitigate his damages.

131. Because of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts to track any fraudulent activity that has occurred and the time it has taken to rectify the fraudulent activity.

---

[38] *See* Notice of Security Incident, (Exhibit A)

132. This time has been lost forever and cannot be recaptured. This time was spent at Defendant's direction by way of the Data Breach notice where Defendant recommended that Plaintiff mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

133. Even with the best response, the harm caused to Plaintiff cannot be undone.

134. Plaintiff suffered actual injury in the form of damages to his credit score as a result of unauthorized credit checks by unknown parties as well as damage and diminution to the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach.

135. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and has constant anxiety and increased concerns for the loss of his privacy.

136. Plaintiff has suffered imminent and impending injury arising from the exacerbated risk of fraud, identity theft, and misuse resulting from their Private Information being placed in the hands of criminals. This is evident by the harm experienced by Plaintiff when his credit score was decreased as a consequence of the hard credit checks on Plaintiff's credit score.

137. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

VII. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

138. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered

inadequate identity monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

139. The credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden on Plaintiff and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

140. Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

141. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

142. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

143. Plaintiff and Class Members were damaged in that their Private Information is in the hands of cyber criminals.

144. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

145. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

146. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

147. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

148. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

149. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

150. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

151. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;
b. Canceling and reissuing credit and debit cards;
c. Purchasing credit monitoring and identity theft prevention;
d. Addressing their inability to withdraw funds linked to compromised accounts;
e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;
h. Contacting financial institutions and closing or modifying financial accounts;
i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and
k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

152. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

153. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

154. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

VIII. CLASS REPRESENTATION ALLEGATIONS

155. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

156. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All persons whose Private Information was compromised because of the March 2024 Data Breach (the "Class").

157. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

158. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery.

159. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23.

160. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiffs now, but Defendant have provided notice to the Office of the Attorney General of Texas that the number includes at least 127,112 individuals.[39]

161. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

[39] State of Texas, Office of the Attorney General, Data Security Breach Report, *available at* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited April 2, 2025)

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was per se negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant was unjustly enriched;

m. Whether Defendant failed to provide notice of the Data Breach promptly; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

162. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant.

Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

163. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

164. Predominance. Defendant have engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

165. Superiority and Manageability. Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

166. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

167. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

168. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

169. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

170. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

171. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect their data systems were reasonable considering best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

172. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

IX. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

173. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

174. Defendant required Plaintiff and Class Members to submit non-public personal information to obtain healthcare services.

175. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

176. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

177. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and their clients current and former patients, which is recognized by laws and regulations, including, but not limited to, HIPAA, as well as common law. Defendant could ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

178. Goodwill owed these duties to Plaintiff and members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols.

179. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or

disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all the healthcare, dental, and/or medical information at issue constitutes "protected health information" within the meaning of HIPAA.

180. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

181. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

182. Defendant breached their duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect timely that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

183. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting protected health information.

184. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

185. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

186. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

187. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT
NEGLIGENCE PER SE
(On Behalf of Plaintiff and All Class Members)

188. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

189. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

190. Under HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

191. Under HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.Defendant breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

192. Defendant breached its duties to Plaintiff and Class Members under North Dakota law by failing to develop and implement policies and procedures necessary to protect Plaintiff's and Class Members' PHI.

193. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

194. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

195. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

by failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

196. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

197. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

198. When Plaintiff and Class Members provided their Private Information to Defendant's client in exchange for healthcare services, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

199. Defendant solicited, offered, and invited, via it's clients, Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members provided their Private Information to Defendant.

200. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and adhered to industry standards.

201. Plaintiff and Class Members paid money, via their medical provider, to Defendant to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

202. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private

Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

203. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

204. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

205. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

206. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

207. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

208. Defendant became guardians of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant and Plaintiff and Class Members.

209. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class

Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

210. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its client's current and former patients, in particular, to keep secure their Private Information.

211. Defendant breached their fiduciary duties by, inter alia, failing to comply with the guidelines outlined under HIPAA and the FTC act for safeguarding and storing it. This failure resulted in the Data Breach that ultimately came to pass.

212. Defendant breached their fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

213. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long

as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

214. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

215. Plaintiff and the Class seek compensatory damages for breach of fiduciary duty, which entails the amount of the difference between the price they paid for defendant's services as promised and the diminished value of its health care services and the costs of future monitoring of their credit history for identity theft and fraud, and/or other damages, plus prejudgment interest and costs.

X. PRAYER FOR RELIEF

216. WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above seek the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiffs and their counsel to represent the Class, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Any other relief that this court may deem just and proper.

XI. JURY TRIAL DEMANDED

217. Plaintiff demands a trial by jury on all claims so triable.

Dated: April 3, 2025

Respectfully submitted,

/s/ Joshua Sanford
Joshua Sanford
Arkansas Bar No. 2001037
SANFORD LAW FIRM
10800 Financial Centre Pkwy, Suite 510
Little Rock, Arkansas 72211
Phone: (501) 221-0088
josh@sanfordlawfirm.com

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
Service only: service@eksm.com
EKSM, LLP
4200 Montrose Street, Suite 200
Houston, Texas 77006
Phone: (888) 350-3931

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS

(* denotes *pro hac vice* forthcoming)